UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/390,362	09/07/1999	SCOTT ALEXANDER VANSTONE	06944.0017	6724

22852	7590	09/08/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _13 July 2005_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-13_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-13_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action. The previous office action(s) is/are incorporated by reference in its/their entirety. The examiner assumes that the applicant agrees with any well-known prior art statements and/or rejections made by the examiner in the previous office action(s) that were not argued. Any objections or rejections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

Claims 1-13 are pending.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

Applicant's arguments filed 7/13/2005 have been fully considered but they are not persuasive.

As per claim 1, applicant argues that McCollom does not teach combining two signature components with a plainttext bit string to create an output signature as claimed in claim 1. The examiner respectfully does not see that limitation recited in claim 1. The closest limitation the examiner sees recited in claim 1 states "combining said first and second component with said other of said bit strings to provide a signature." It is unclear from the wording of the claim if said first and second components refer to the signature components or if "said" might have been a typo and

applicant may have meant "a first and second component." Looking at the previous

examiner's rejections, the examiner sees that column 3, lines 11-20 of McCollom was

cited for the rejection of this limitation. The examiner submits that the signal combiner

combining one or more of the data components and at least one first level digital

signature into a signal which then gets encrypted and signed reads on the limitation of

"combining said first and second component with said other of said bit strings to provide

a signature."

As per claim 1, applicant argues there is no suggestion in McCollom of sending a

portion of a message "in the clear" as plaintext to be used as an input in the verification

process. The examiner does not see this limitation recited in claim 1 and assumes that

limitation being argued may have been disclosed in the specification. Applicant is

reminded that although the claims are interpreted in light of the specification, limitations

from the specification are not read into the claims. See *In re Van Geuns*, 988

F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As per claim 7, applicant argues neither McCollom nor Kitaori teach using a

portion of plaintext to verify a message that has been subdivided. The examiner does

not see this limitation recited in claim 7 and assumes that limitation being argued may

have been disclosed in the specification. Applicant is reminded that although the claims

are interpreted in light of the specification, limitations from the specification are not read

into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.

1993).

Applicant's other arguments are directed towards the other references used in

the rejections do not provide what applicant believed were missing from McCollam and

Kitaori above and are moot as the examiner has shown that the limitations being argued

aren't recited in the claims. Applicant's other arguments directed towards dependent

claims being allowable because the independent claims are allowable are also moot.

The previous examiner's rejections of the claims are repeated below for record.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, 7, 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable

over McCollom (EP0918274A2) in view of Kitaori et al (5915024).

With respect to Claim 1, the limitation "subdividing said message into a pair of bit

strings" is met by McCollom on column 7, lines 28-40. McCollom reveals the message

being used to create a digital signature comprises of one ore more components and

furthermore goes into manipulation of one or more message components on column 4,

lines 41-42, 45-47. Further limitation of "utilizing one of said bit strings to compute a

first signature component, forming from said first signature component and another of

said bit strings an intermediate signature component... and combining first and second

components with said other of said bits strings to provide a signature" is met by

McCollom, column 3, lines 11-20. Please note that the word "fingerprint" in McCollom

refers to "signature" as stated on column 1, lines 21-23. McCollom describes

manipulation of data components to create the digital signature on page 3, lines 11-14.

McCollom however does not disclose a public and private key encryption explicitly even

though he does mention on column 4, lines 50-52 that any suitable encryption algorithm

can be used.

Further limitation of "utilizing said intermediate component and said private key to

provide a second signature component" is met by Kitaori on Fig. 8.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine the teachings of Kitaori within the system of McCollom so as to be able to

preserve the integrity of the message being sent and furthermore prevent repudiation of

the message by the sender.

With respect to Claim 6, all the limitation is met by McCollom and Kitaori et al

except the limitation disclosed below.

The limitation of "wherein said second component is generated by hashing said

first component and said other bit string" is met by Kitaori et al on Fig. 21. It would have

been obvious to one of ordinary skill in the art at the time the invention was made to

incorporate the teachings of Kitaori et al within the system of McCollom because

message hashing is a necessary step in the creation of a digital signature.

With respect to Claim 7, the limitation "including at least one component having only one of said bit strings encrypted therein, and the other of said bit strings, said method comprising the steps of combining said one component with the other bit string, recovering said one bit string from said combination" is met by McCollom, column 3, lines 11-20.

The limitation "examining said recovered one bit string for a predetermined characteristic" is inherent in McCollom, column 3, lines 11-20.

The limitation "a method of verifying a message subdivided into a pair of bit strings from a signature" is met by McCollom on column 7, lines 30-40. This reference shows that the message is composed of one or more data components that are manipulated. Hence manipulation of two data components is met by the teaching.

McCollom however does not describe the usage of the information of the signer towards the digital signature process. Kitaori discusses this as described below.

The limitation "using publicly available information of the purported signer" is met by Kitaori et al on column 9, lines 28-30.

It would be obvious to one of ordinary skill in the art at the time the invention was made to combine Kitaori's teaching within the system of McCollom as to preserve the validity of the message, as discussed in Kitaori et al on column 8, lines 61-65.

With respect to Claim 11, all the limitation is met by McCollom except the limitation disclosed below.

The limitation of "wherein said first signature component is formed by applying a function to said one of said bit strings and said one of said bit strings may be recovered from said signature component by applying a complementary function to said signature component" is met by Kitaori et al on Fig. 19.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kitaori et al within the system of McCollom because encryption and decryption of the sent message is useful in preventing an attacker from being able to decipher the converted message.

With respect to Claim 12, all the limitation is met by McCollom except the limitation disclosed below.

The limitation of "wherein said function is encryption with a key, said key is recoverable from said signature, and said complementary function is decryption with said key" is met on Fig. 8 and 12.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kitaori et al within the system of McCollom because encryption and decryption of the sent message is useful in preventing an attacker from being able to decipher the converted message.

With respect to Claim 13, all the limitation is met by McCollom except the limitation disclosed below.

The limitation of "wherein said key is a short-term public key derived from a

short-term private key used in the provision of said second signature component" is met

on Fig. 12.

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to combine the teachings of Kitaori et al within the system of

McCollom because asymmetric encryption is a well known method used in the creation

of digital signatures, whereby a private key is used to encrypt the message being sent.

Likewise a public key is needed to decrypt the encrypted message received.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCollom

(EP0918274A2) in view of Kitaori et al (5915024) in view of Menezes et al (Handbook of

Applied Cryptography) in further view of Nyberg (0639907A1).

The combination of McCollom and Kitaori et al is already discussed in Claim 1

rejection. The combination of McCollom and Kitaori et al does not describe any

redundancy being introduced into the message. Menezes however discusses

redundancy in a message being transmitted. Menezes describes comparing message

redundancy within a message to a checksum, which is some form of predetermined

level. Furthermore, Nyberg teaches on page 2, column2, lines 48-49 that validation of a

message x can be based on some redundancy contained in x.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to incorporate Menezes's teaching of redundancy into the combination of

McCollom and Kitaori et al teaching because of Nyberg's motivation that suggests that

redundancy bits help with message validation.

Claims 3, 4, 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over

McCollom (EP0918274A2) in view of Kitaori et al (5915024) in further view of Menezes

et al (Handbook of Applied Cryptography) in further view of Nyberg (0639907A1) in

further view of ISO/IEC FCD 9796-1.

With regards to Claim 3, the combination of McCollom, Kitaori et al, Menezes

and Nyberg have already been discussed in Claim 2 rejection. The combination of

McCollom, Kitaori et al, Menezes and Nyberg however do not teach about redundancy

being introduced to exceed a predetermined level. The limitation "wherein said

redundancy is adjusted to exceed said predetermined level" is taught by ISO/IEC FCD

9697-1 on page1, third paragraph, lines 12-14. The reference talks about the message

being extended, which represents the excess bits that exceed the predetermined level.

Redundancy being introduced into the message is also further discussed in the

reference.

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to add the teachings of ISO/IEC FCD 9697-1 to the combination of

McCollom, Kitaori et al, Menezes and Nyberg because the excess bits help in the

verification process, where the redundancy needs to be revealed (ISO/IEC FCD 9796-1,

page 1, third paragraph, lines 16-18), so that the message can be eventually retrieved.

With regards to Claim 4, the combination of McCollom, Kitaori et al, Nyberg and ISO/IEC FCD 9796-1 do not discuss data being added to the message for the purpose of adjusting the redundancy. However, Menezes inherently discloses this on page 363, first paragraph. It would have been obvious to one of ordinary skill in the art at the time of the invention to implement redundancy in the message teaching of Menezes within the combination of McCollom, Kitaori et al, Nyberg and ISO/IEC FCD 9796-1 because incorporation of redundancy bits into a message assists with message validation (Nyberg, page 2, column2, lines 48-49).

With regards to Claim 5, the combination of McCollom, Kitaori et al, Menezes and Nyberg do not discuss an indicator for showing that data has been added to the message. However this is inherent in the reference ISO/IEC FCD 9697-1 on page1, third paragraph, lines 16-18. Since redundancy in the message needs to be revealed by the verification process, there is inherently an indicator that would shows this. It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of ISO/IEC FCD 9697-1 to the combination of McCollom, Kitaori et al, Menezes and Nyberg because the detection of the redundancy bits in the message is necessary for message validation as taught by Nyberg on page 2, column2, lines 48-49, and it further helps in the telling apart the message from the redundancy bits so that the message can be eventually extracted.

Claims 8, 9, 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

McCollom (EP0918274A2) in view of Kitaori et al (5915024) in further view of Nyberg

(0639907A1)

With regards to Claim 8, the combination of McCollom and Kitaori do not

expressly disclose hashing of the signal component and bit string. Even though

McCollom does not discuss hashing, he talks about encryption of the combined signal

on column 3, lines 17-18. Nyberg, furthermore, expressly discusses hashing in digital

signatures on column 2, lines 49-56. Hence, hashing can be intuitively substituted for

the encryption step in McCollom since it is a form of an encryption process, and

furthermore, a necessary part of obtaining a digital signature.

It would be obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the hashing teaching of Nyberg within the combination of McCollom and

Kitaori's system because hashing is a necessary, common step in the process of

obtaining a digital signature.

With regards to Claim 9, the combination of McCollom, Kitaori and Nyberg have

been discussed in Claim 8. However, the combination of McCollom and Kitaori does

not describe redundancy as part of the digital signature process. Nyberg however

discusses this as shown below.

The limitation "wherein said predetermined characteristic is the redundancy of

said recovered one bit string" is met by Nyberg, column 2, lines 48-49. It would have

been obvious to one of ordinary skill in the art at the time the invention was made to add

the teachings of Nyberg to the combination of McCollom and Kitaori because

redundancy is very useful for message validation.

With regards to Claim 10, all the limitation have already been met by the

combination of McCollom, Kitaori and Nyberg as already discussed in Claim 9. The

limitation of "said signature includes a second component derived from a combination of

said one component and said other bit string and said one bit string is recovered

utilizing said second component" is met by McCollom, column 3, lines 11-20.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time
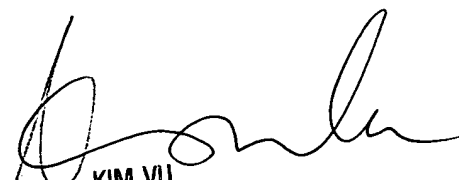
policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-

7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100